PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-158654

(43)Date of publication of application : 31.05.2002

---

(51)Int.Cl. H04L 9/16
H04L 9/08
H04N 7/167

---

(21)Application number : 2000-351510 (71)Applicant : HITACHI LTD

(22)Date of filing : 17.11.2000 (72)Inventor : OWADA TORU
KITAHARA JUN
ASAHI TAKESHI

---

(54) INFORMATION PROCESSOR, DISPLAY DEVICE, DIGITAL CONTENTS DISTRIBUTION SYSTEM AND DIGITAL CONTENTS DISTRIBUTION/ OUTPUT METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To enable the final output of digital contents in a form to stimulate audio and visual desires of a user, while protecting rights of the digital contents.

SOLUTION: An information processor body 102 transfers the digital contents (display data) encoded by using an encoding key information 105 to be shared with a display device 103 to the display device 103 and the display device 103 performs a decoding processing to the display data to be transferred from the information processor body 102

by using the encoding key information 105. The display data to be transferred from the information processor body 102 to the display device 103 here is one, the only a part of which is encoded, for example, and every piece of display data for several lines is encoded every several lines.

LEGAL STATUS [Date of request for examination] 28.01.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] In the information processor equipped with the processor and the output unit at least the above-mentioned processor A cipher-processing means to perform cipher processing to a digital content using the cryptographic key information shared with the above-mentioned output unit, It has a transfer means to transmit the enciphered digital content to the above-mentioned output unit. The above-mentioned output unit An input means to input the digital content transmitted from the above-mentioned processor, The information processor characterized by having a decode processing means to perform decode processing using the cryptographic key information shared with the above-mentioned processor, and an output means to output the digital content after decoding an encryption part, to the inputted digital content.

[Claim 2] In the information processor equipped with the processor and the output unit at least the above-mentioned processor A cipher-processing means to perform cipher processing to a part of digital content using the cryptographic key information shared with the above-mentioned output unit, It has a transfer means to transmit the digital content as which the part was enciphered to the above-mentioned output unit. The above-mentioned output unit An input means to input the digital content transmitted from the above-mentioned processor, The information processor characterized by having a decode processing means to perform decode processing using the cryptographic key information shared with the above-mentioned processor, and an output means to output the digital content after decoding an encryption part, to the inputted digital content.

[Claim 3] In the information processor equipped with the processor and the output unit at least the above-mentioned processor As opposed to the digital content inputted as an input means to input the enciphered digital content A decode processing means to perform decode processing using the cryptographic key information for decoding this digital content, A cipher-processing means to perform cipher processing to a part of digital content after decode using the cryptographic key information shared with the above-mentioned output unit, It has a transfer means to transmit the enciphered digital content to the above-mentioned output unit. The above-mentioned output unit An input means to input the digital content transmitted from the above-mentioned processor, The information processor characterized by having a decode processing means to perform decode processing using the

cryptographic key information shared with the above-mentioned processor, and an output means to output the digital content after decoding an encryption part, to the inputted digital content.

[Claim 4] The information processor characterized by to have an input means input the enciphered digital content, a decode processing means perform decode processing using the cryptographic key information for decoding this digital content to the digital content which inputted, a cipher-processing means perform cipher processing to a part of digital content after decode using the cryptographic key information which shares with the output unit of the output destination change of this digital content, and a transfer means transmit the digital content as which a part was enciphered to the above-mentioned output unit.

[Claim 5] It is the information processor which it is an information processor according to claim 3 or 4, and the digital content which the above-mentioned input means inputs makes one unit the formatting unit of the digital content at the time of a plaintext, and is characterized by being enciphered as some units of these units serve as a candidate for encryption.

[Claim 6] It is the information processor characterized by being an information processor according to claim 2, 3, 4, or 5, and for the above-mentioned cipher-processing means making one unit the formatting unit of the digital content at the time of a plaintext, and performing cipher processing for some units of these units as a processing object of cipher processing.

[Claim 7] It is the information processor which the above-mentioned cipher-processing means makes one unit voice data for two or more samples about the voice data outputted to the above-mentioned voice regenerative apparatus when it is an information processor according to claim 2, 3, 4, or 5 and the above-mentioned output unit is a voice regenerative apparatus, and is characterized by performing cipher processing for some units of these units as a processing object of cipher processing.

[Claim 8] When it is an information processor according to claim 2, 3, 4, or 5 and the above-mentioned output unit is a display, the above-mentioned cipher-processing means In the direction of Rhine of the indicative data outputted to the above-mentioned indicating equipment, the indicative data for two or more lines is made into one unit. Some units of these units as a processing object of cipher processing The information processor which makes one unit the indicative data for two or more columns in the direction of a column of the indicative data which performs cipher processing or is outputted to the above-mentioned indicating

equipment, and is characterized by performing cipher processing for some units of these units as a processing object of cipher processing.

[Claim 9] It is the information processor which the above-mentioned cipher-processing means makes one unit the data for 1 pixel of the indicative data outputted to the above-mentioned indicating equipment when it is an information processor according to claim 2, 3, 4, or 5 and the above-mentioned output unit is an indicating equipment, and is characterized by performing cipher processing for the part as a processing object of cipher processing respectively about a part or all of these units.

[Claim 10] The display characterized by having an input means to input the enciphered indicative data, a decode processing means to perform decode processing to the inputted indicative data using the cryptographic key information shared with the information processor of the source of this indicative data, and a display means to display the indicative data after decoding an encryption part.

[Claim 11] The digital content which is an indicating equipment according to claim 10, and the above-mentioned input means inputs [whether in the direction of Rhine of the indicative data at the time of a plaintext, as the indicative data for two or more lines is made into one unit and some units of these units serve as a processing object of cipher processing, it is enciphered, and] Or the display which makes one unit the indicative data for two or more columns in the direction of a column of the indicative data at the time of a plaintext, and is characterized by being enciphered as some units of these units serve as a processing object of cipher processing.

[Claim 12] It is the display which is an information processor according to claim 10, and the digital content which the above-mentioned input means inputs makes one unit the data for 1 pixel of the indicative data at the time of a plaintext, and is characterized by enciphering it respectively about a part or all of these units as the part serves as a processing object of cipher processing.

[Claim 13] In the digital content distribution system equipped with the digital content distribution equipment which distributes a digital content, and the information processor which transmits and outputs the digital content distributed from digital content distribution equipment to an output unit the above-mentioned digital content distribution equipment An are recording means by which the digital content as which the part was enciphered using the 1st cryptographic key information shared with the above-mentioned information processor is accumulated, It has a distribution means to distribute the accumulated digital content to the above-mentioned information processor. The above-mentioned information processor An input means to input the

digital content distributed from the above-mentioned digital content distribution equipment, A decode processing means to perform decode processing to the encryption part in the inputted digital content using the cryptographic key information on the above 1st, A cipher-processing means to perform cipher processing to a part of digital content after decoding an encryption part using the 2nd cryptographic key information shared with the above-mentioned output unit, It has a transfer means to transmit the enciphered digital content to the above-mentioned output unit. The above-mentioned output unit An input means to input the digital content transmitted from the above-mentioned information processor, A decode processing means to perform decode processing to the encryption part in the inputted digital content using the cryptographic key information on the above 2nd, It has an output means to output the digital content after decoding an encryption part. The cipher-processing means of the above-mentioned digital content distribution equipment, and the cipher-processing means of the above-mentioned information processor The digital content distribution system which makes one unit the formatting unit of the digital content at the time of a plaintext, and is characterized by performing cipher processing for some units of these units as a processing object of cipher processing. [Claim 14] In the digital content distribution system equipped with the digital content distribution equipment which distributes a digital content, and the information processor which transmits and outputs the digital content distributed from digital content distribution equipment to an output unit It is the approach of distributing a digital content to the above-mentioned information processor from the above-mentioned digital content distribution equipment, and outputting with the above-mentioned output unit. The above-mentioned digital content distribution equipment the digital content as which the part was enciphered using the 1st cryptographic key information shared with the above-mentioned information processor As opposed to the encryption part in the digital content to which it distributes to the above-mentioned information processor, and the above-mentioned information processor is distributed from the above-mentioned digital content distribution equipment Perform decode processing using the cryptographic key information on the above 1st, and a part of digital content after decoding an encryption part is received. After performing cipher processing using the 2nd cryptographic key information shared with the above-mentioned output unit As opposed to the encryption part in the digital content to which the digital content after encryption is transmitted to the above-mentioned output unit, and the above-mentioned output unit is transmitted from the above-mentioned information

processor Perform decode processing using the cryptographic key information on the above 2nd, and that of the digital content after decoding an encryption part is outputted. The digital content which the above-mentioned digital content distribution equipment distributes, and the digital content which the above-mentioned information processor transmits The digital content distribution and the output method which makes one unit the formatting unit of the digital content at the time of a plaintext, and is characterized by being enciphered as some units in these units serve as a candidate for encryption.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention distributes a digital content and relates to the approach of outputting with the information processor of a distribution place, enabling use in the form which stimulates audiovisual desire of the user who prevents the unauthorized use by the duplicate especially, and does not have a just use right about the technique of treating the digital content which needs protection of copyrights.

[0002]

[Description of the Prior Art] recent years, an image, voice, etc. -- high -- the demand which distributes added value information by the digital format is increasing, and in order to plan the protection of copyrights of a digital content, importance has

been attached to prevention of an illegal copy. That is, since quality does not deteriorate even if it copies when it can copy easily, evils, such as infringement of the copyright by the illegal copy, are already producing a digital content.

[0003] Encryption of a digital content is used, and only the user who received just cryptographic key information decodes the enciphered digital content, and enables it to confirm the contents generally as one of the anti-copying means.

[0004]

[Problem(s) to be Solved by the Invention] If there is no just cryptographic key information, it will become impossible however, to completely view and listen to the enciphered digital content, when a digital content is enciphered simply.

[0005] This is because it becomes impossible for the software and hardware which the DS of a digital content will be destroyed and reproduce a digital content to completely interpret DS by performing simple encryption which disregarded the format, in spite of formatting the digital content according to a certain format.

[0006] Then, unless a user purchases a digital content and just cryptographic key information comes to hand, the contents will not be able to be confirmed but the threshold of digital content purchase will become high for a user.

[0007] Although right protection of a digital content is made into a major premise in order to solve such a problem, it is desirable to distribute a digital content in the form which stimulates audiovisual desire of a user.

[0008] Moreover, conventionally, encryption of a digital content is performed only about the path until it reaches a user's information processor, and is not set as the object of the protection of copyrights by encryption in the information processor about the path at the time of outputting to final output equipments, such as a display.

[0009] Since the final output equipment of a digital input like a liquid crystal display is becoming common in recent years instead of the final output equipment of an analog input like the conventional CRT (Cathode-Ray Tube) indicating equipment, there is a possibility that the illegal copy of a digital content may be performed, in the path at the time of outputting to such final output equipment.

[0010] Then, the purpose of this invention is in an information processor to make it possible to prevent the illegal copy in the path at the time of finally outputting a digital content.

[0011] Moreover, in an information processor, another purpose of this invention is by stimulating audiovisual desire of a user to make it possible to promote distribution or sale of contents at the time of digital one while protecting the right of a digital content.

[0012]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, this invention transmits the digital content which the above-mentioned processor enciphered using the cryptographic key information shared with the above-mentioned output unit in the information processor equipped with the processor and the output unit at least to the above-mentioned above-mentioned output unit, and the above-mentioned output unit is made to perform decode processing to the digital content transmitted from the above-mentioned processor using the above-mentioned cryptographic key information.

[0013] And especially, in order to attain another purpose, the digital content transmitted to the above-mentioned output unit from the above-mentioned processor makes one unit the formatting unit of the digital content at the time of a plaintext, and they are made to be enciphered in this invention, as some units of these units serve as a candidate for encryption.

[0014]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained with reference to a drawing.

[0015] Drawing 1 is the outline block diagram of the digital content distribution system concerning this operation gestalt.

[0016] For 100, as for an information processor and 102, digital content distribution equipment and 101 are [the body of an information processor and 103] displays among drawing.

[0017] The digital content distribution system concerning this operation gestalt makes the major premise right protection of the high added value contents distributed as digital data by digital content distribution equipment 100. That is, the digital content (distribution data) by which between digital content distribution equipment 100 and the bodies 102 of an information processor is transmitted to the digital content distribution system concerning this operation gestalt, and the digital content (indicative data) to which between the body 102 of an information processor and indicating equipments 103 is transmitted are aiming at protection by having enciphered these for what is digital data respectively.

[0018] And the digital content distribution system concerning this operation gestalt aims at enabling distribution of a digital content in the form which stimulates audiovisual desire of a user. That is, the digital content distribution system concerning this operation gestalt is the enciphered digital content, and makes it possible to stimulate an audiovisual demand of a user.

[0019] Specifically, the digital content to which between digital content distribution

equipment 100 and the bodies 102 of an information processor is transmitted is encryption data enciphered with the cipher system with which the digital data formatted by compression methods decided beforehand, such as JPEG (Joint Photographic Experts Group) and MPEG (Moving Picture Experts Group), was decided [DES / (Data Encryption Standard)] beforehand.

[0020] Here, even if digital content distribution equipment 100 is network equipment which distributes a digital content via a network, it may be the record medium with which digital contents, such as an optical disk medium and a magnetic-disk medium, were recorded, for example.

[0021] That is, digital content distribution equipment 100 may not perform cipher processing that it should just be enciphered when the digital content distributed by digital content distribution equipment 100 is distributed from digital content distribution equipment 100.

[0022] Now, as shown in drawing 1 , it sets to the digital content distribution system concerning this operation gestalt, and digital content distribution equipment 100 and the body 102 of an information processor have the function to share the cryptographic key information 104 for enciphering / decrypting a digital content (distribution data) by a certain approach.

[0023] About the approach of sharing the cryptographic key information 104, various approaches serve as a well-known technique, and what kind of approach may be adopted.

[0024] For example, the approach the body 102 of an information processor receives the cryptographic key information 104 is mentioned from the network equipment which has managed the cryptographic key information 104 used for encryption of a digital content. Network equipment enciphers the cryptographic key information 104 using the public key information on the body 102 of an information processor, and it is made for the body 102 of an information processor to decode for the private key information on own at this time.

[0025] Moreover, the method of recording the cryptographic key information 104 used for encryption of the digital content (finishing [encryption]) currently recorded on the magnetic-disk medium, for example on the nonvolatile storage inside the body 102 of an information processor at the time of manufacture of the body 102 of an information processor is mentioned.

[0026] Similarly, as shown in drawing 1 , it sets to the digital content distribution system concerning this operation gestalt, and the body 102 of an information processor and the indicating equipment 103 have the function to share the

cryptographic key information 105 for enciphering / decrypting a digital content (indicative data) by a certain approach.

[0027] Also about the approach of sharing the cryptographic key information 105, like the approach of sharing the cryptographic key information 104, various approaches serve as a well-known technique, and what kind of approach may be adopted.

[0028] For example, the approach a display 103 receives the cryptographic key information 105 which the body 102 of an information processor used for encryption of a digital content from the body 102 of an information processor is mentioned. The body 102 of an information processor enciphers the cryptographic key information 105 using the public key information on a display 103, and it is made for a display 103 to decode for the private key information on own at this time.

[0029] Moreover, for example, the method of recording the cryptographic key information 105 on the nonvolatile storage of each interior at the time of manufacture of the body 102 of an information processor and a display 103 is mentioned.

[0030] Moreover, as shown in drawing 1 , it sets to the digital content distribution system concerning this operation gestalt. As opposed to the encryption part in the digital content to which the body 102 of an information processor is distributed from (1) digital-content distribution equipment 100 The decode function to perform decode processing 106 using the cryptographic key information 104, the expansion function to perform expansion processing 107 of the digital content after decoding (2) encryption parts, (3) As opposed to a part of the display-control function and (4) indicative datas which perform display-control processing 108 changed into the indicative data for outputting the developed digital content with the bit rate which an indicating equipment 103 requires It has the code function to perform cipher processing 109 using the cryptographic key information 105.

[0031] Moreover, as shown in drawing 1 , in the digital content distribution system concerning this operation gestalt, the display 103 has the decode function to perform decode processing 110 using the cryptographic key information 105, and the display function which performs display processing 111 of the indicative data after decoding (2) encryption parts to the encryption part in the indicative data enciphered by the code function of the body 102 of (1) information processor.

[0032] Next, outline actuation of the digital content distribution system concerning this operation gestalt is explained using drawing 2 .

[0033] Drawing 2 is the outline operation flow chart of the digital content distribution system concerning this operation gestalt.

[0034] Setting to drawing 2 , digital content distribution equipment 100 and the body

102 of an information processor first share the cryptographic key information 104 for enciphering / decrypting a digital content (distribution data) by a certain approach (step 201). Since various approaches serve as a well-known technique about the approach of sharing the cryptographic key information 104 and what kind of approach may be adopted as mentioned above, it does not specify here.

[0035] Then, digital content distribution equipment 100 distributes the digital content as which the part was enciphered using the cryptographic key information 104 to the body 102 of an information processor (step 202). As mentioned above, digital content distribution equipment 100 may not perform cipher processing that what is necessary is to just be enciphered when the digital content distributed by digital content distribution equipment 100 is distributed from digital content distribution equipment 100.

[0036] Then, the body 102 of an information processor performs decode processing 106 using the cryptographic key information 104 to the encryption part in the digital content distributed from digital content distribution equipment 100 (step 203). By processing of step 203, the body 102 of an information processor will obtain the digital content of a plaintext to the interior.

[0037] Then, the body 102 of an information processor performs expansion processing 107 of the digital content obtained by processing of step 203 (step 204). For example, when the digital content obtained by processing of step 203 is MPEG data formatted by the MPEG method, the body 102 of an information processor will obtain the dynamic-image data which become the interior from per second 30 frames by processing of step 204.

[0038] Then, display-control processing 108 for outputting with the bit rate which an indicating equipment 103 requires to the indicative data containing the dynamic-image data obtained by processing of step 204 is performed (step 205). For example, when a display 103 is a TFT (Thin FilmTransistor) liquid crystal display, in processing of step 205, the body 102 of an information processor generates the sequential indicative data of about per second 60-70 frames.

[0039] Then, the body 102 of an information processor and an indicating equipment 103 share the cryptographic key information 105 for enciphering / decrypting a digital content (indicative data) by a certain approach (step 206). Since various approaches serve as a well-known technique about the approach of sharing the cryptographic key information 105 and what kind of approach may be adopted as mentioned above, it does not specify here.

[0040] Then, the body 102 of an information processor performs cipher processing

109 to the part in the indicative data generated by processing of step 205 using the cryptographic key information 105 (step 207). By processing of step 207, the body 102 of an information processor will obtain the indicative data as which the part was enciphered by the interior.

[0041] Then, the body 102 of an information processor outputs the indicative data as which the part was enciphered to an indicating equipment 103 (step 208).

[0042] Then, an indicating equipment 103 performs decode processing 110 using the cryptographic key information 105 to the encryption part in the indicative data outputted from the body 102 of an information processor (step 209). By processing of step 209, an indicating equipment 103 will obtain the indicative data of a plaintext to the interior.

[0043] Then, an indicating equipment 103 performs display processing 111 of the indicative data obtained by processing of step 209 (step 210). The indicative data which contains the dynamic-image data obtained by processing of step 204 by processing of step 210 will be displayed.

[0044] As mentioned above, the digital content distributed from digital content distribution equipment 100 will be displayed by processing of step 201 - step 210 with a display 103.

[0045] In addition, below, the actuation realized by processing of step 201 - step 204 among actuation of the digital content distribution system concerning this operation gestalt is called "distribution path encryption" actuation, and the actuation realized by processing of step 205 - step 210 is called "output path encryption" actuation.

[0046] Moreover, even if processing of step 206 is performed in advance of distribution path encryption actuation, it may be carried out in parallel. Moreover, depending on the configuration of an information processor 101, sequence may reverse processing of step 205, step 206, and step 207.

[0047] Next, the detail of distribution path encryption actuation is explained.

[0048] First, outline actuation of the information processor 101 concerning this operation gestalt is explained using drawing 3 .

[0049] Drawing 3 is the outline block diagram of the information processor 101 concerning this operation gestalt.

[0050] By drawing 3 , it is a part about a display among the information processors 101, such as a personal computer (PC), and only the part about distribution path encryption actuation is shown.

[0051] the inside of drawing, and 102 -- the body of an information processor, and 103 -- a display and 104 -- cryptographic key information and 301 -- a central processing

unit (CPU:Central Processing Unit) and 302 -- a system memory and 303 -- for an input control unit and 306, as for a bus and 308, the CCE and 307 are [a display control and 304 / display memory and 305 / the decode processing section and 309] the contents expansion processing sections.

[0052] In drawing 3 , when digital content distribution equipment 100 is network equipment, CCE 306 inputs a digital content according to directions of CPU301. Moreover, when digital content distribution equipment 100 is a record medium, an input control unit 305 inputs a digital content according to directions of CPU301. The digital content which CCE 306 or an input control unit 305 inputted is inputted into a display control 303 through a bus 307 according to directions of CPU301.

[0053] In a display control 303, the decode processing section 308 performs decode processing 106 to the encryption part in the inputted digital content using the cryptographic key information 104 currently held inside the display control 303, and obtains the digital content of a plaintext inside a display control 303. Then, the contents expansion processing section 309 performs expansion processing 107 of a digital content which the decode processing section 308 decoded, and obtains the digital content developed inside the display control 303.

[0054] The actuation so far is equivalent to distribution path encryption actuation. About the detail of subsequent output path encryption actuation, it mentions later.

[0055] In addition, the decode processing section 308 and the contents expansion processing section 309 may be made to be mounted in a display control 303 as hardware, and prepare CPU and memory original in a display control 303, and may be made to be mounted as software.

[0056] Next, distribution path encryption actuation explains an example of the encryption approach of the digital content distributed from digital content distribution equipment 100 using drawing 5 and drawing 6 .

[0057] Drawing 5 is the explanatory view showing an example of the encryption approach of the digital content distributed from digital content distribution equipment 100, and drawing 6 is the explanatory view showing the display image at the time of displaying the digital content enciphered by the encryption approach shown in drawing 5 with an indicating equipment 103.

[0058] In drawing 5 and drawing 6 , the case where a digital content is MPEG data is made into the example.

[0059] An one-frame mxn pixel and the dynamic-image data which consist of per second k frames are classified into three formats, I picture format, P picture format, and B picture format, according to compression by the MPEG method, for example.

[0060] (1) In an I picture formal I picture format, after the image data of an one-frame mxn pixel is divided into two or more 8x8-pixel blocks, and orthogonal transformation processing is performed for every block and changed into frequency-domain data, it quantizes and a data compression is performed. In I picture data, coding only for the data in a former frame is made, and one frame data are obtained from I picture data by expansion processing.

[0061] (2) In a P picture formal P picture format, the data compression which performed inter-frame prediction of the forward direction is performed. P picture data -- difference with I picture -- coding using information is made and P picture data and I picture data used as former drawing are needed for restoration of a former frame. That is, image data is not obtained only with P picture data.

[0062] (3) In a B picture formal B picture format, the data compression which performed bidirectional inter-frame prediction is performed. B picture data -- the difference between I picture and P picture -- coding using information is made and P picture data, I picture data used as former drawing, and B picture data are needed for restoration of a former frame. That is, image data is not obtained only with B picture data.

[0063] Moreover, the sign allotment of one picture data becomes small in order of I picture, P picture, and B picture, as shown in drawing 5 . Dynamic-image data are encoded in sequence, such as IBB, PBB, PBB, IBB, PBB, and PBB, for every frame.

[0064] The following three approaches can be considered as the MPEG data encryption approach with such a property.

[0065] (1) As the encryption approach of the 1st encryption approach 1st, there is a method of enciphering only I picture data. The 1st encryption approach is further divided into the approach of enciphering for every high frequency field data / low frequency field data of /Not giving, paying attention to the frequency component within the approach of enciphering for every block used as a compression unit of /Not giving, and the block used as a compression unit.

[0066] First, if the former approach (the approach of enciphering for every block used as a compression unit of /not giving) is explained, in case encryption by this approach will be performed, for example to the former image shown in drawing 6 (a), a block is made into the processing object of cipher processing, cipher processing is performed to a certain block, and it is made not to perform cipher processing to a certain block.

[0067] If the MPEG data enciphered by this approach do not perform decode processing which used the cryptographic key information 104, the image at the time of being displayed on an indicating equipment 103 comes to be shown in drawing 6 (b). By

this approach, by making the block count which enciphers fluctuate, it is controllable in the dirt degree of a former image, and can change freely what indication is performed.

[0068] Next, if the latter approach (the approach of enciphering for every high frequency field data / low frequency field data of /not giving) is explained, in case encryption by this approach will be performed, for example to the former image shown in drawing 6 (a), the low frequency field data within a block are made into the processing object of cipher processing, cipher processing is performed to the low frequency field data under each block, and it is made not to perform cipher processing to high frequency field data. If the MPEG data enciphered by this approach do not perform decode processing which used the cryptographic key information 104, the image at the time of being displayed on an indicating equipment 103 comes to be shown in drawing 6 (c).

[0069] Although it will not illustrate if high frequency field data are enciphered, although it will become difficult for a former image to be polluted greatly and to observe a former image as shown in drawing 6 (c) if low frequency field data are enciphered, it becomes the image superimposed on the noise by the former image.

[0070] By this approach, by choosing the frequency domain which enciphers, it is controllable in the dirt degree of a former image, and can change freely what indication is performed. Moreover, even if it does not make all blocks into the processing object of cipher processing, it is good also considering a part of blocks as a processing object of cipher processing.

[0071] when only I picture data is enciphered by the 1st encryption approach, and there is no cryptographic key information 104, I picture data cannot be restored, therefore it is shown in drawing 5 -- as -- the difference of I picture data -- P picture data and B picture data which are information also become impossible [also developing these], although not enciphered. For example, when there are no dynamic-image data of 104 cryptographic key information encoded in order of IBB, PBB, PBB, IBB, PBB, and PBB, it becomes xxx, xxx, xxx, xxx, xxx, and xxx (x means failure in normal decode and expansion.), and a former image with all normal frames is not obtained.

[0072] (2) As the encryption approach of the 2nd encryption approach 2nd, there is a method of enciphering only P picture data. The 2nd encryption approach is also further divided into the approach of enciphering for every high frequency field data / low frequency field data of /Not giving, like the 1st encryption approach paying attention to the frequency component within the approach of enciphering for every

block used as a compression unit of /Not giving, and the block used as a compression unit.

[0073] when only P picture data is enciphered by the 2nd encryption approach, and there is no cryptographic key information 104, P picture data cannot be restored, therefore it is shown in drawing 5 -- as -- the difference of I picture data and P picture data -- B picture data which is information also becomes impossible [also developing this], although not enciphered. For example, the dynamic-image data of 104 cryptographic key information encoded in order of IBB, PBB, PBB, IBB, PBB, and PBB become Ixx, xxx, xxx, Ixx, xxx, and xxx (x means failure in normal decode and expansion.), when there is nothing, and the normal image frame obtained serves as only I picture data.

[0074] (3) As the encryption approach of the 3rd encryption approach 3rd, there is a method of enciphering only B picture data. The 3rd encryption approach is also further divided into the approach of enciphering for every high frequency field data / low frequency field data of /Not giving, like the 1st encryption approach paying attention to the frequency component within the approach of enciphering for every block used as a compression unit of /Not giving, and the block used as a compression unit.

[0075] When only B picture data is enciphered by the 3rd encryption approach, if there is no cryptographic key information 104 as shown in drawing 5 , B picture data cannot be restored. For example, the dynamic-image data of 104 cryptographic key information encoded in order of IBB, PBB, PBB, IBB, PBB, and PBB become Ixx, Pxx, Pxx, Ixx, Pxx, and Pxx (X means failure in normal decode and expansion.), when there is nothing, and the normal image frame obtained serves as only I picture data and P picture.

[0076] As mentioned above, although three approaches were explained as the MPEG data encryption approach, you may make it combine these approaches with arbitration.

[0077] Since a digital content is not enciphered simply, but the data made into the processing object of cipher processing are chosen in distribution path encryption actuation and he is trying to encipher only a part according to the digital content distribution system concerning this operation gestalt, when it does not have the just cryptographic key information 104, it will be in the condition that some former images were stained. Since it becomes possible since the value is spoiled to prevent the illegal copy of a digital content and a part of digital content is indicated, the digital content with which the part was soiled stimulates a viewing-and-listening demand of a user, and becomes possible [urging perfect viewing and listening of a digital content].

[0078] In case the data made into the processing object of cipher processing are

chosen, he is trying to pay his attention to the format in the digital content distribution system especially applied to this operation gestalt. Namely, although it will be completely impossible for all the DS called the header, the payload, and footer to be lost, and to use as a digital content when it considers as the processing object of cipher processing by making a digital content into a mere bit string In the digital content distribution system concerning this operation gestalt Since he is trying to choose the data which do not treat a digital content as a mere bit string, but are made into the processing object of cipher processing according to the significant taste part of a format, not the whole data but a part of dirt is possible.

[0079] Moreover, since cipher processing which used the cryptographic key information 104 for data dirt is used in distribution path encryption actuation, in order to stimulate viewing-and-listening desire of a user according to the digital content distribution system concerning this operation gestalt, it is not necessary to prepare a dirt digital content apart from a perfect digital content, and becomes that it is possible to reduce the cost concerning distribution and are recording of a digital content.

[0080] Furthermore, according to the digital content distribution system concerning this operation gestalt, in distribution path encryption actuation, mitigation of the throughput of cipher processing / decode processing is also possible by making a part of digital content into the processing object of cipher processing, and avoiding cipher processing to the whole digital content. In addition, whenever [dirt], and throughput have the relation of a trade-off, and modification of a priority is easily possible according to a demand.

[0081] It becomes possible to stimulate viewing-and-listening desire of a user, protecting copyright on the distribution path of a digital content by distribution path encryption actuation according to the digital content distribution system concerning this operation gestalt, as explained above.

[0082] In addition, the information processor 101 concerning this operation gestalt is made the configuration shown in drawing 7 instead of the configuration shown in drawing 3 , and software may be made to realize the decode processing section 308 and the contents expansion processing section 309 which were shown in drawing 3 .

[0083] Drawing 7 is other outline block diagrams of the information processor 101 concerning this operation gestalt.

[0084] Like [drawing 7] drawing 3 , it is a part about a display among the information processors 101, such as PC, and only the part about distribution path encryption actuation is shown.

[0085] The same sign is given among drawing to the same component as drawing 3 .

701 is a nonvolatile storage.

[0086] In the information processor 101 of a configuration of being shown in drawing 7 , CPU301 realizes actuation of the decode processing section 308 shown in drawing 3 , and the contents expansion processing section 309 by loading a program and performing on a system memory 302.

[0087] In drawing 7 , when digital content distribution equipment 100 is network equipment, CCE 306 inputs a digital content according to directions of CPU301. Moreover, when digital content distribution equipment 100 is a record medium, an input control unit 305 inputs a digital content according to directions of CPU301. The digital content which CCE 306 or an input control unit 305 inputted is inputted into a system memory 302 through a bus 307 according to directions of CPU301.

[0088] To the encryption part in the inputted digital content, CPU301 performs decode processing 106 using the cryptographic key information 104, and obtains the digital content of a plaintext on a system memory 302. Then, CPU301 performs decoded expansion processing 107 of a digital content, and obtains the developed digital content. The obtained digital content is inputted into a display control 303.

[0089] Here, by explanation which used drawing 3 , although held inside a display control 303, in the information processor 101 of a configuration of being shown in drawing 7 , as for the cryptographic key information 104, CPU301 shall also realize sharing of the cryptographic key information 104 by loading and performing a program on a system memory 302.

[0090] Moreover, also in any of drawing 3 and drawing 7 , although the information processor 101 concerning this operation gestalt is considered as the configuration equipped with information-processor 102 body and the display 103, it may be the configuration which the body 102 of an information processor and the display 103 unified. That is, it is good also as a Personal Digital Assistant called the so-called PDA (PersonalDigital Assistant) etc. in the information processor 101 concerning this operation gestalt.

[0091] Generally, since a Personal Digital Assistant is constituted using CPU with the comparatively low engine performance, the memory of small capacity, etc. in many cases, cipher processing which is comparatively heavy processing has the problem of becoming a big burden for a Personal Digital Assistant.

[0092] Then, if a Personal Digital Assistant with such a problem is used by the digital content distribution system concerning this operation gestalt, when coexistence of the audiovisual desire stimulus of protection of copyrights and a user which this invention makes the purpose by treating the digital content as which not the whole but

the part was enciphered is realizable, the load fall effectiveness by reduction of code throughput can be acquired. When a Personal Digital Assistant realizes cipher processing by software especially, it becomes unnecessary to carry highly efficient CPU and a highly efficient bulk memory in cipher processing, and effectiveness, such as low-cost-izing and low-power-izing, is acquired. Moreover, since processing speed required for the hardware only for cipher processing falls when a Personal Digital Assistant is equipped with the hardware only for cipher processing, effectiveness, such as low-power-izing by the low working speed and low-cost-izing by small-scale-izing of hardware logic, is acquired.

[0093] By the way, in above-mentioned explanation, although MPEG data (dynamic-image data) were made into the example, it is not necessarily aimed only at dynamic-image data.

[0094] For example, when a digital content is JPEG data (static-image data), it is possible to use the encryption approach of I picture data mentioned above and the same encryption approach.

[0095] Moreover, what is necessary is to perform band division to speech information, to be made to perform encryption only to the encryption/high frequency component only to a low-frequency component, or just to carry out as [encipher / every number sample], for example, since divided coding which became independent for every frequency component is performed when a digital content is MPEG data (voice data). Thus, if whenever [data dirt] is controlled, it will become possible to generate a jarring playback sound moderately.

[0096] Now, the detail of output path encryption actuation is explained below.

[0097] First, outline actuation of the information processor 101 concerning this operation gestalt is explained using drawing 4 .

[0098] Drawing 4 is the outline block diagram of the information processor 101 concerning this operation gestalt.

[0099] By drawing 4 , it is a part about a display among the information processors 101, such as PC, and only the part about output path encryption actuation is shown.

[0100] The same sign is given among drawing to the same component as drawing 3 . As for the cipher-processing section and 402, 401 is [the decode processing section and 403] data drivers.

[0101] Here, let displays 103 be for example, liquid crystal display (LCD:Liquid Crystal Display) equipment and a display of a digital input like the CRT (Cathode-RayTube) equipment possessing a digital to analog function.

[0102] In drawing 4 , the indicative data (plaintext indicative data) containing the

digital content developed inside the display control 303 is accumulated in display memory 304 by the distribution path encryption actuation mentioned above according to directions of CPU301.

[0103] In a display control 303, the plaintext indicative data accumulated in display memory 304 is inputted, and the cipher-processing section 401 performs cipher processing 109 to a part of inputted plaintext indicative data using the cryptographic key information 105 currently held inside the display control 303, and obtains the indicative data enciphered inside the display control 303. The obtained encryption indicative data is inputted into a display 103 from a display control 303.

[0104] Then, in an indicating equipment 103, the decode processing section 402 performs decode processing 110 to the encryption part in the inputted encryption indicative data using the cryptographic key information 105 currently held inside the indicating equipment 103, and obtains a plaintext indicative data inside an indicating equipment 103. Then, the data driver 403 performs display processing 111 of a plaintext indicative data by supplying the plaintext indicative data which the decode processing section 402 decoded to each display pixel on a display screen.

[0105] The above actuation is equivalent to output path encryption actuation.

[0106] In addition, the cipher-processing section 402 may be made to be mounted in a display control 303 as hardware, and prepares CPU and memory original in a display control 303, and may be made to be mounted as software.

[0107] Next, outline actuation of the display control 303 concerning this operation gestalt is explained using drawing 8 .

[0108] Drawing 8 is the outline block diagram of the display control 303 concerning this operation gestalt.

[0109] Drawing 8 shows only the part about output path encryption actuation among display controls 303.

[0110] 801 among drawing the timing generation section and 803 for a memory control section and 802 A timing signal, 804 a memory address signal and 304 for a memory control signal and 805 Display memory, 806 a LCD control signal and 808 for a LCD control section and 807 A plaintext indicative data, 809 a LCD indicative data and 811 for a timing control section and 810 A serial/parallel-conversion circuit (S/P circuit), For an encryption S/P finishing LCD indicative data and 814, as for an encryption LCD indicative data and 816, a parallel/serial-conversion circuit (P/S circuit) and 815 are [812 / a S/P finishing LCD indicative data and 813 / a delay circuit and 817] delayed LCD control signals.

[0111] In drawing 8 , using the timing signal 803 sent from the timing generation

section 802, the memory control section 801 generates the memory control signal 804 and the memory address signal 805, and reads the plaintext indicative data 808 from display memory 304 one by one.

[0112] On the other hand, the LCD control section 806 generates the LCD control signal 807 which controls the display timing of LCD using the timing signal 803 sent from the timing generation section 802.

[0113] The timing control section 809 sends out the plaintext indicative data 809 read from display memory 304 as a LCD indicative data 810 according to the display timing by the LCD control signal 807.

[0114] That is, the plaintext indicative data 808 read from display memory 304 turns into the LCD indicative data 810 which synchronized with the LCD control signal 807 by the timing control section 809.

[0115] For example, supposing the LCD control signal 807 transmits the indicative data for 1 pixel by 1 data-transfer clock synchronization and consists of data whose 1 pixel is 16 bits, the LCD indicative data 810 will serve as a 16-bit data bus. Here, when a block cipher like DES is used for cipher processing, the cipher-processing section 401 will perform block cipher processing of 64 bitwises using the cryptographic key information 105.

[0116] In order to absorb the difference in both batch, in the display control 303 concerning this operation gestalt, the S/P circuit 812 and the P/S circuit 814 are used. The S/P circuit 811 is the data width of face (here) of the LCD indicative data 810. About 16 bitwises, it is a code batch (here). It is what changes into 64 bitwise width of face, and is supplied to the cipher-processing section 401 as a S/P finishing LCD indicative data 812. Moreover, the P/S circuit 814 The data width of face of the encryption S/P finishing LCD indicative data 813 after cipher processing was performed by the cipher-processing section 401 is changed into the data width of face of the LCD indicative data 810, and is supplied to the data driver 403 as an encryption LCD indicative data 815.

[0117] According to the data width of face of the LCD indicative data 810, and the code batch width of face of the cipher-processing section 401, the configurations of the S/P circuit 811 and the P/S circuit 814 differ.

[0118] In the display control 303 applied to this operation gestalt as shown in drawing 8 Since processing by the S/P circuit 811, the cipher-processing section 401, and the P/S circuit 814 is prepared By making it output delay equivalent to delay by these processings as a delayed LCD control signal 817 by the delay circuit 816 in addition to the LCD control signal 807 which the LCD control section 806 generated The

encryption LCD indicative data 816 outputted is made to be supplied to the data driver 403 from the P/S circuit 814 synchronizing with the delayed LCD control signal 817.

[0119] Thereby, creation of the encryption LCD indicative data 815 based on performing cipher processing to a part of indicative data on the way of [of the display timing control by the display control 303 / processing], i.e., real-time cipher processing of the LCD indicative data 810, is attained.

[0120] Next, outline actuation of the display 103 concerning this operation gestalt is explained using drawing 9 .

[0121] Drawing 9 is the outline block diagram of the display 103 concerning this operation gestalt.

[0122] By drawing 9 , the case where a display 103 is a liquid crystal display is made into the example, and only the part (namely, liquid crystal drive drain side driver equivalent to the data driver 403) about output path encryption actuation is shown among displays 103.

[0123] A latch circuit -3,912 is a liquid crystal drive circuit where 901 generate the timing signal (CL1 signal) with which the incorporation signal (CL2 signal) of an encryption indicative data and 902 output an encryption indicative data, and 903 outputs LCD driver voltage, and the voltage level for [904] a liquid crystal drive in the power source for a LCD drive, the level shifter to which a latch circuit -2,909 carries out a liquid crystal drive output signal and 906 to a latch address selector, and 907 carries out the pressure up of the latch circuit -1,908 for 905 from circuit driver voltage to liquid crystal driver voltage and 910 among drawing, 911 is a plaintext indicative data

[0124] In drawing 9 , the latch address selector 906 is counting falling of CL2 signal 901 (it is equivalent to the delayed LCD control signal 817 shown in drawing 8 .) inputted from the display control 303 synchronizing with the input of the encryption indicative data 902, and generates the latch signal over a latch circuit -1 (907).

[0125] The encryption indicative data 902 inputted from the display control 303 is held on the latch circuit -1 (907) at entry sequence by the latch signal which the latch address selector 906 generates.

[0126] CL1 signal 903 is a Horizontal Synchronizing signal inputted for every display of one line, and the encryption indicative data 902 for 1 display Rhine latched by the input of CL1 signal 903 on the latch circuit -1 (907) is latched on every one-line latch circuit -2 (908) for every one-line display period.

[0127] Decode processing 100 which used the cryptographic key information 105 is

performed by the decode processing section 402, and the encryption indicative data 902 for one line latched on the latch circuit -2 (908) turns into the plaintext indicative data 912, and is latched on every one-line latch circuit -3 (911) for every one-line display period by CL1 signal 903.

[0128] The plaintext indicative data 912 for one line latched on the latch circuit -3 (911) is changed into liquid crystal driver voltage through a level shifter 909 and the liquid crystal drive circuit 910, and is impressed to an one-line display period and liquid crystal.

[0129] By the above processing, the display action to liquid crystal is performed for every line.

[0130] When a block cipher like DES is used for decode processing, only the part in which parallel processing is possible makes coincidence arrange in parallel the number of bits to which the decode processing section 402 is outputted from a latch circuit -2 (908) per block here. For example, since a liquid crystal drive drain side driver will become 18432 bits per line supposing it is a 18-bit output per pixel with the 1024-pixel configuration per line, 288 blocks of 64 bitwises (batch by DES) are made to arrange in parallel. And the decode processing section 402 will perform block decode processing of 64 bitwises using the cryptographic key information 105.

[0131] Thereby, creation and a display of the plaintext indicative data 912 based on performing decode processing to a part of indicative data on the way of [of the display control by the liquid crystal drive drain side driver of an indicating equipment 103 / processing], i.e., real-time decode processing of the encryption indicative data 912, are attained.

[0132] In addition, the display 103 concerning this operation gestalt may be made the configuration shown in drawing 10 instead of the configuration shown in drawing 9 .

[0133] Drawing 10 is other outline block diagrams of the display 103 concerning this operation gestalt.

[0134] Drawing 10 as well as drawing 9 makes the example the case where a display 103 is a liquid crystal display, and only the part (namely, liquid crystal drive drain side driver equivalent to the data driver 403) about output path encryption actuation is shown among displays 103.

[0135] The same sign is given among drawing to the same component as drawing 9 . For 1001, as for a P/S circuit and 1003, a S/P circuit and 1002 are [a S/P finishing indicative data and 1004] plaintext indicative datas.

[0136] The indicating equipment 103 shown in drawing 10 the data width of face of the encryption indicative data 902 When it differs from the data width of face of the

decode batch of the decode processing section 402 depending on the number of data bits and data transfer clock (CL2 signal 901) per pixel, by the S/P circuit 1001 After changing the data width of face of the encryption indicative data 902 into the data width of face of a suitable decode batch and considering as the S/P finishing indicative data 1003, by the decode processing section 402 Decode processing is performed using the cryptographic key information 105, and the plaintext indicative data 1004 obtained by decode processing is changed into the data width of face of the plaintext indicative data 912 by the P/S circuit 1002.

[0137] You may make it the decode processing section 402 make a processing block arrange in parallel according to the number of bits of the encryption indicative data 902 per pixel, and CL2 signal 901 that what is necessary is just to be able to process at least 1 block.

[0138] As mentioned above, although the case where a display 103 was a liquid crystal display was taken for the example and output path encryption actuation was explained, if it is made to perform same decode processing on the way which performs digital processing even when a display 103 is CRT equipment which possesses the digital to analog section by the digital input, creation and a display of a plaintext indicative data will be attained.

[0139] Next, output path encryption actuation explains an example of the encryption approach of the indicative data outputted from a display control 303 using drawing 11 and drawing 12 .

[0140] Drawing 11 is the explanatory view showing an example of the encryption approach of the indicative data outputted from a display control 303, and is the explanatory view showing the display image at the time of displaying the enciphered indicative data with an indicating equipment 103.

[0141] Drawing 11 shows the encryption approach of performing cipher processing in the direction of Rhine, and the encryption approach of performing cipher processing in the direction of a column, as the encryption approach of a former image (original plaintext indicative data).

[0142] (1) In case encryption by this approach is performed to the encryption approach (original plaintext indicative data), for example, the former image shown in drawing 11 (a), of performing cipher processing in the direction of Rhine, in the direction of Rhine, the indicative data for two or more lines (for example, about several lines) is made into one unit, and be made to perform cipher processing for some units of these units as a processing object of cipher processing. It is made to repeat the case where the case where cipher processing is performed, and cipher processing are

not specifically performed by turns for every indicative data for several lines.

[0143] If the indicative data enciphered by this approach performs decode processing which used the cryptographic key information 105, the image at the time of being displayed on an indicating equipment 103 will turn into the same image as the former image shown in drawing 11 (a), but if decode processing using the cryptographic key information 105 is not performed, the image at the time of being displayed on an indicating equipment 103 serves as the indicative data with which several lines were soiled at intervals of several lines, as shown in drawing 11 (b).

[0144] The number of Rhine made into one unit is determined beforehand, and while the cipher-processing section 401 of a display control 303 enciphers alternatively for every number of determined Rhine, it is made for the decode processing section 402 of a display 103 to decode alternatively by this approach. The dirt to a part of indicative data is attained by this, and it becomes reducible [the code / decode throughput in the cipher-processing section 401 of a display control 303, and the decode processing section 402 of a display 103].

[0145] Moreover, by making the number of Rhine made into one unit fluctuate, it is controllable in the dirt degree of an indicative data, and can change freely what indication is performed.

[0146] (2) In case encryption by this approach is performed to the encryption approach (original plaintext indicative data), for example, the former image shown in drawing 11 (a), of performing cipher processing in the direction of a column, in the direction of a column, the indicative data for two or more columns (for example, number column extent) is made into one unit, and be made to perform cipher processing for some units of these units as a processing object of cipher processing. It is made to repeat the case where the case where cipher processing is performed, and cipher processing are not specifically performed by turns for every indicative data for a number column.

[0147] If the indicative data enciphered by this approach performs decode processing which used the cryptographic key information 105, the image at the time of being displayed on an indicating equipment 103 will turn into the same image as the former image shown in drawing 11 (a), but if decode processing using the cryptographic key information 105 does not perform, the image at the time of being displayed on an indicating equipment 103 serves as the indicative data with which a part for a number column was soiled every number column, as shown in drawing 11 (c).

[0148] The number of columns made into one unit is determined beforehand, and while the cipher-processing section 401 of a display control 303 enciphers alternatively for

every number of the determined columns, it is made for the decode processing section 402 of a display 103 to decode alternatively by this approach. The dirt to a part of indicative data is attained by this, and it becomes reducible [the code / decode throughput in the cipher-processing section 401 of a display control 303, and the decode processing section 402 of a display 103].

[0149] Moreover, by making the number of columns made into one unit fluctuate, it is controllable in the dirt degree of an indicative data, and can change freely what indication is performed.

[0150] Drawing 12 is the explanatory view showing an example of the encryption approach of the indicative data outputted from a display control 303, and shows the encryption approach of performing cipher processing to the part about the indicative data for 1 pixel in a former image (original plaintext indicative data), by drawing 12 .

[0151] By this approach, it is made to perform cipher processing only to the high order bit in the indicative data in 1 pixel, or made to perform cipher processing only to the lower bit in the indicative data in 1 pixel.

[0152] Only a high order bit is enciphered, and when a lower bit is considered as as [plaintext], the variation of an indicative data becomes large. Then, if it displays on an indicating equipment 103, without decoding an encryption indicative data, whenever [dirt / of data] will be large and observation of an indicative data will become difficult.

[0153] Moreover, when only a lower bit is enciphered and a high order bit considers as as [plaintext], there is little variation of an indicative data. Then, although whenever [dirt / of data] will be small and will be observed as a flicker on a screen if it displays on an indicating equipment 103, without decoding an encryption indicative data, rough observation of an indicative data is possible.

[0154] By drawing 12 , the indicative data for 1 pixel consisted of 8 bits, and when a certain plaintext indicative data was "55h", the example from which only the high order bit was enciphered, "55h" turned into "e5h", only the lower bit was enciphered, and "55h" turned into "52h" was shown. Thus, since the variation from a plaintext indicative data becomes large, the direction which enciphers only a high order bit will be observed as a more different display.

[0155] By this approach, it becomes it can be possible to choose the dirt degree of an indicative data, and reducible [the code / decode throughput in the cipher-processing section 401 of a display control 303, and the decode processing section 402 of a display 103] by choosing whether only a high order bit is enciphered or only a lower bit is enciphered.

[0156] As mentioned above, although the encryption approach of performing cipher

processing in the direction of Rhine / the direction of a column, and the encryption approach of performing cipher processing only to the high order bit/lower bit in the indicative data in 1 pixel were explained, you may make it combine these approaches with arbitration.

[0157] According to the digital content distribution system concerning this operation gestalt, the protection of copyrights of the digital content in the output path to the indicating equipment 103 which is final output equipment which was not performed becomes possible conventionally by output path encryption actuation.

[0158] And since a digital content (indicative data) is not enciphered simply, but the data made into the processing object of cipher processing are chosen in output path encryption actuation and he is trying to encipher only a part according to the digital content distribution system concerning this operation gestalt, when it does not have the just cryptographic key information 105, it will be in the condition that some former images were stained. Since it becomes possible since the value is spoiled to prevent the illegal copy of a digital content and a part of digital content is indicated, the digital content with which the part was soiled stimulates a viewing-and-listening demand of a user, and becomes possible [urging perfect viewing and listening of a digital content].

[0159] Furthermore, according to the digital content distribution system concerning this operation gestalt, in output path encryption actuation, mitigation of the throughput of cipher processing / decode processing is also possible by making a part of digital content into the processing object of cipher processing, and avoiding cipher processing to the whole digital content. In addition, whenever [dirt], and throughput have the relation of a trade-off, and modification of a priority is easily possible according to a demand.

[0160] It becomes possible to stimulate viewing-and-listening desire of a user, protecting copyright on the output path of a digital content by output path encryption actuation according to the digital content distribution system concerning this operation gestalt, as explained above.

[0161] In addition, the information processor 101 concerning this operation gestalt is made the configuration shown in drawing 13 instead of the configuration shown in drawing 4 , and software may be made to realize the cipher-processing section 401 shown in drawing 4 .

[0162] Drawing 13 is other outline block diagrams of the information processor 101 concerning this operation gestalt.

[0163] Like [drawing 13] drawing 4 , it is a part about a display among the information processors 101, such as PC, and only the part about output path encryption actuation

is shown.

[0164] The same sign is given among drawing to the same component as drawing 4 . 701 is a nonvolatile storage.

[0165] In the information processor 101 of a configuration of being shown in drawing 13 , CPU301 realizes actuation of the cipher-processing section 401 shown in drawing 4 by loading a program and performing on a system memory 302. That is, he is trying, as for the information processor 101 of a configuration of being shown in drawing 13 , for not the display control 303 but CPU301 to encipher an indicative data.

[0166] Drawing 14 is the explanatory view showing outline actuation of the information processor 101 of a configuration of being shown in drawing 13 .

[0167] As shown in drawing 14 , the plaintext indicative data 808 accumulated in display memory 304 is inputted into a system memory 302 through a display control 303 and a bus 307 according to directions of CPU301.

[0168] CPU301 performs cipher processing 109 to the inputted plaintext indicative data 808 using the cryptographic key information 105. the encryption indicative data 902 enciphered by CPU301 is boiled and inputted into display memory 304 through a bus 307 and a display control 303. The encryption indicative data 902 accumulated in display memory 304 is read by the display control 303, and is outputted to a display 103.

[0169] That is, in the information processor 101 of a configuration of being shown in drawing 13 , CPU301 generates the plaintext indicative data 808 on display memory 304, and generates the encryption indicative data 902 on display memory 304 from the plaintext indicative data 808 further. A display control 303 performs read-out actuation of the encryption indicative data 902, and performs a display action.

[0170] Here, although the cryptographic key information 105 shall be held inside a display control 303 by the explanation which used drawing 4 , in the information processor 101 of a configuration of being shown in drawing 13 , the cryptographic key information 105 shall be held at the nonvolatile storage 701.

[0171] Moreover, in any of drawing 4 and drawing 13 , although the information processor 101 concerning this operation gestalt is considered as the configuration equipped with information-processor 102 body and the display 103, as distribution path encryption actuation explained, it may be the configuration which the body 102 of an information processor and the display 103 unified. That is, it is good also as a Personal Digital Assistant called the so-called PDA etc. in the information processor 101 concerning this operation gestalt.

[0172] Since a Personal Digital Assistant is generally constituted using CPU with the

comparatively low engine performance, the memory of small capacity, etc. in many cases as mentioned above, cipher processing which is comparatively heavy processing has the problem of becoming a big burden for a Personal Digital Assistant.

[0173] Then, if a Personal Digital Assistant with such a problem is used by the digital content distribution system concerning this operation gestalt, when coexistence of the audiovisual desire stimulus of protection of copyrights and a user which this invention makes the purpose by treating the digital content as which not the whole but the part was enciphered is realizable, the load fall effectiveness by reduction of code throughput can be acquired. When a Personal Digital Assistant realizes cipher processing by software especially, it becomes unnecessary to carry highly efficient CPU and a highly efficient bulk memory in cipher processing, and effectiveness, such as low-cost-izing and low-power-izing, is acquired. Moreover, since processing speed required for the hardware only for cipher processing falls when a Personal Digital Assistant is equipped with the hardware only for cipher processing, effectiveness, such as low-power-izing by the low working speed and low-cost-izing by small-scale-izing of hardware logic, is acquired.

[0174] By the way, in above-mentioned explanation, although the output to a digital display unit was made into the example, it is not necessarily aimed only at the display.

[0175] For example, also in an audio output device with a digital input, it is possible to realize output unit path encryption actuation by enciphering every number sample similarly to the voice data by which PCM (Pulse CodeModulation) coding was carried out.

[0176] When it does not have just cryptographic key information because it is made to perform cipher processing in the form depending on a format of a digital content to a part of digital content, he is trying for the digital content distribution system concerning this operation gestalt to serve as a digital content with which the part was soiled, as explained above. Then, it becomes possible to stimulate audiovisual desire of a user, protecting the copyright of a digital content.

[0177] Therefore, according to the digital content distribution system concerning this operation gestalt, it becomes possible to circulate the high digital content of added value on a semi-conductor storage or a digital network safely, and becomes applicable to digital content distribution service etc.

[0178] In addition, in protection of a digital content, it is good also as a system using either distribution path encryption actuation or the output path encryption actuation, and good also as a system which combines both and protects a digital content with two independent cipher systems.

[0179]

[Effect of the Invention] The final output of a digital content which can stimulate audiovisual desire of a user becomes possible, protecting the copyright of a digital content according to this invention, as explained above.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The outline block diagram of the digital content distribution system concerning this operation gestalt.

[Drawing 2] The outline operation flow chart of the digital content distribution system concerning this operation gestalt.

[Drawing 3] The outline block diagram of the information processor concerning this operation gestalt.

[Drawing 4] The outline block diagram of the information processor concerning this operation gestalt.

[Drawing 5] The explanatory view showing an example of the encryption approach of the digital content distributed from digital content distribution equipment.

[Drawing 6] The explanatory view showing the display image at the time of displaying the digital content enciphered by the encryption approach shown in drawing 5 with an indicating equipment.

[Drawing 7] The outline block diagram of the information processor concerning this operation gestalt.

[Drawing 8] The outline block diagram of the display control concerning this operation gestalt.
[Drawing 9] The outline block diagram of the display concerning this operation gestalt.
[Drawing 10] The outline block diagram of the display concerning this operation gestalt.
[Drawing 11] The explanatory view showing an example of the encryption approach of the indicative data outputted from a display control.
[Drawing 12] The explanatory view showing an example of the encryption approach of the indicative data outputted from a display control.
[Drawing 13] The outline block diagram of the information processor concerning this operation gestalt.
[Drawing 14] The explanatory view showing outline actuation of the information processor shown in drawing 13 .
[Description of Notations]
100: Digital content distribution equipment
101: Information processor
102: The body of an information processor
103: Display
104: Cryptographic key information
105: Cryptographic key information
106: Decode processing
107: Contents expansion processing
108: Display-control processing
109: Cipher processing
110: Decode processing
111: Display processing
301: Central processing unit (CPU:Central Processing Unit)
302: System memory
303: Display control
304: Display memory
305: Input control unit
306: Communication controller
307: Bus
308: Decode processing section
309: Contents expansion processing section
401: Cipher-processing section

402: Decode processing section
403: Data driver
701: Nonvolatile storage
801: Memory control section
802: Timing generation section
803: Timing signal
804: Memory control signal
805: Memory address signal
806: LCD (Liquid Crystal Display) control section
807: LCD control signal
808: Plaintext indicative data
809: Timing control section
810: LCD indicative data
811: Serial/parallel-conversion circuit (S/P circuit)
812: S/P finishing LCD indicative data
813: Encryption S/P finishing LCD indicative data
814: Parallel/serial-conversion circuit (P/S circuit)
815: Encryption LCD indicative data
816: Delay circuit
817: Delayed LCD control signal
901: CL2 signal
902: Encryption indicative data
903: CL1 signal
904: The power source for a LCD drive
905: Liquid crystal drive output signal
906: Latch address selector
907: Latch circuit -1
908: Latch circuit -2
909: Level shifter
910: Liquid crystal drive circuit
911: Latch circuit -3
912: Plaintext indicative data
1001: S/P circuit
1002: P/S circuit
1003: S/P finishing indicative data
1004: Plaintext indicative data